Finite Fields and Their Applications 18 (2012) 271–282

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Binomial and factorial congruences for $\mathbb{F}_q[t]$

Dinesh S. Thakur [1]

Department of Mathematics, University of Arizona, Tucson, AZ 85721, USA

ARTICLE INFO

Article history:
Received 18 May 2011
Revised 22 August 2011
Accepted 23 August 2011
Available online 8 September 2011
Communicated by Arne Winterhof

In memory of late Bhimsen Joshi

MSC:
11T55
11R58
11B65
11A07

Keywords:
Function fields
Carlitz module
Bernoulli numbers

ABSTRACT

We present several elementary theorems, observations and questions related to the theme of congruences satisfied by binomial coefficients and factorials modulo primes (or prime powers) in the setting of polynomial ring over a finite field. When we look at the factorial of n or the binomial coefficient 'n choose m' in this setting, though the values are in a function field, n and m can be usual integers, polynomials or mixed. Thus there are several interesting analogs of the well-known theorems of Lucas, Wilson etc. with quite different proofs and new phenomena.

1. Introduction

Many strong analogies [4,6] between number fields and function fields over finite fields have been used to benefit the study of both. These analogies are even stronger in the base case $\mathbb{Q}, \mathbb{Z} \leftrightarrow \mathbb{F}_q(t), \mathbb{F}_q[t]$. We will explore congruences satisfied by analogs of factorials and binomial coefficients. When we look at the factorial of n or the binomial coefficient 'n choose m' in this setting, though the values are in function field, n and m can be usual integers, polynomials or mixed. Thus we will see several interesting analogs of the well-known theorems of Lucas, Wilson etc. We refer to [6, Chapter 4] for historical references, properties of these analogs and proofs of many things recalled here.

E-mail address: thakur@math.arizona.edu.

[1] Supported in part by NSA grant H98230-10-1-0200.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2011.08.003

Let us fix the basic standard notation.

$\mathbb{Z}$	{integers}
$\mathbb{F}_q$	a finite field of q elements, q a power of prime p
A	the polynomial ring $\mathbb{F}_q[t]$, t a variable over $\mathbb{F}_q$
K	the function field $\mathbb{F}_q(t)$
A_+	{monics (in t) in A}
A_d	{elements of A of degree d}
$[n]$	$= t^{q^n} - t$
D_n	$= \prod_{i=0}^{n-1}(t^{q^n} - t^{q^i}) = \prod[n-i]^{q^i}$
L_n	$= \prod_{i=1}^{n}(t^{q^i} - t) = \prod[i]$
$e_k(x)$	$= \prod(x-a)$, where $a \in A$ runs through elements of degree $< k$
$\mathcal{N}a$	$= q^d$ for $a \in A_d$, i.e., the norm of a
$\wp$	a monic irreducible polynomial in A of degree d
$v(n)$	highest k such that $\mathcal{N}\wp^k$ divides n

We use the standard convention that empty sums are zero and the empty products are one, so that $D_0 = L_0 = 1$.

2. Multiple analogs

For $n \in \mathbb{Z}$, $n \geqslant 0$, we define the **first factorial** (due to Carlitz) by

$$n! := \prod D_i^{n_i} \in A_+, \quad \text{for } n = \sum n_i q^i,\ 0 \leqslant n_i < q.$$

See [6, 4.5–4.8, 4.12, 4.13] for its properties, such as prime factorization, divisibilities, functional equations, interpolations and arithmetic of special values, which are analogous to those of the classical factorial. See also [1,2], which gives many interesting divisibility properties in great generality, in particular, applying to the first factorial and to the first and the third binomials below. (The usual factorial with values in $\mathbb{Z}$ will be always mentioned as the classical factorial.)

For $x \in A$, with $-x$ not monic, we define the **second factorial** by

$$\Pi(x) := \prod_{a \in A+} \left(1 + \frac{x}{a}\right)^{-1} \in K.$$

See [6, 4.9–4.13] for its analogous properties such as the location of poles (in $-A_+$), functional equations, interpolations at all primes and arithmetic of special values etc. Its reciprocal is integral! Note also that we basically excluded $q = 2$ with the conditions on x. (The usual binomial with values in $\mathbb{Z}$ will be always mentioned as the classical binomial.)

For $n, m \in \mathbb{Z}$, $n, m \geqslant 0$, we define the **first binomial coefficient** by

$$\binom{n}{m} := \frac{n!}{m!(n-m)!} \in A_+, \quad \text{if } n \geqslant m,\ 0 \text{ otherwise.}$$

See [6, 4.13–4.15] for its analogous properties regarding divisibilities.

For $a, b \in A$, with $-a$, $-b$ not monic, we define the **second binomial coefficient** by

$$\begin{bmatrix} a \\ b \end{bmatrix} := \frac{\Pi(a)}{\Pi(b)\Pi(a-b)} \in K, \quad \text{if } b - a \text{ not monic},\ 0 \text{ otherwise.}$$

For $a \in A$, $n \in \mathbb{Z}$, $n \geqslant 0$, we define the **third binomial coefficient** by

$$\left\{ \begin{matrix} a \\ n \end{matrix} \right\} := \prod \left\{ \begin{matrix} a \\ q^i \end{matrix} \right\}^{n_i} \in A, \quad \text{where } \left\{ \begin{matrix} x \\ q^k \end{matrix} \right\} := \sum x^{q^i} (-1)^{k-i} / \left(D_i L_{k-i}^{q^i} \right),$$

where n_i are the base q digits of n as above. See [6, 4.13–4.15] for analogous properties of this definition, due to Carlitz, its use Mahler type interpolation in results of Wagner etc.

We now record some results [6, Chapter 2] we will use often. (III)–(V) and (VII) are due to Carlitz.

(I) $[n]$ is the product of monic irreducible polynomials in A of degree dividing n.
(II) $(D_0 D_1 \cdots D_{d-1})^{q-1} = D_d / L_d$.
(III) D_n is the product of monic polynomials in A of degree n.
(IV) L_n is the (monic) least common multiple of polynomials in A of degree n.
(V) $\{ \begin{smallmatrix} x \\ q^k \end{smallmatrix} \} = e_k(x)/D_k$, and thus equals 0 (1 respectively), if $x \in A$ is of degree less than (monic of degree equal to) k.
(VI) $\Pi(a)^{-1} = \prod_{i=0}^{d} (1 + \{ \begin{smallmatrix} a \\ q^i \end{smallmatrix} \})$, if $a \in A_d$, with $-a$ not monic.
(VII) If $C_a(z) = \sum \{ \begin{smallmatrix} a \\ q^i \end{smallmatrix} \} z^{q^i}$, then $C_{ab}(z) = C_a(C_b(z)) = C_{ba}(z)$. (Note C_a is the famous Carlitz module, but we will not need any more of its related theory.)

3. Results of Lucas type

The well-known theorem of Lucas expresses the classical binomial coefficient 'm choose n' modulo a prime p as the product of 'm_i choose n_i', where m_i, n_i are the base p digits of m, n respectively. In our case, the modulus is a prime $\wp$ of the function field, and we get several versions, with digits for the base $\wp$ or $\mathcal{N}\wp$, according to which binomial we use.

Theorem 3.1. *Let $\wp$ be a prime of A of degree d. Then we have*

$$\binom{m}{n} \equiv \prod \binom{m_i(d)}{n_i(d)} \mod \wp,$$

where $m = \sum m_i(d) q^{di}$ and $n = \sum n_i(d) q^{di}$ are the base q^d-expansions of m and n respectively, so that $0 \leqslant m_i(d), n_i(d) < q^d$.

In particular, the binomial is zero modulo $\wp$ if and only if there is a carry over of q^d-digits in the sum $n + (m - n)$, i.e., $n_i(d) > m_i(d)$ for some i.

Proof. First observe that if there is no carry over of base q-digits, then all the binomial coefficients above are equal to one, because of the digit expansion definition of first factorial. Now suppose there is a carry over at (base q) exponents $i, i+1, \ldots, j-1$, but not at $i-1$ or j. Let $\sum m_k q^k$, $\sum n_k q^k$ and $\sum \ell_k q^k$ be the base q expansions of m, n, $m-n$ respectively. Then $n_k + \ell_k$ is $m_i + q$, $m_k + q - 1$ or $m_j - 1$ according as whether k is i, $i+1 \leqslant k \leqslant j-1$ or $k = j$. Thus, using the digit expansion and the definition of the factorials, we see that the contribution of this block of digits to the binomial coefficient expression is

$$\frac{D_j}{D_{j-1}^{q-1} \cdots D_{i+1}^{q-1} D_i^q} = [j] \cdots [i].$$

On the other hand, the congruence class of $[k]$ modulo $\wp$ depends on the congruence class of k modulo d, and both are zero if d divides k. □

Theorem 3.2. *Let $\wp$ be a prime of A of degree d. Then we have*

$$\left\{ \begin{matrix} a \\ n \end{matrix} \right\} \equiv \prod \left\{ \begin{matrix} a_i \\ n_i(d) \end{matrix} \right\} \mod \wp,$$

where $a = \sum a_i(d)\wp^i$ ($n = \sum n_i(d)q^{di}$ *respectively*) *is the base* $\wp$- ($q^d = \mathcal{N}\wp$ *respectively*)*-expansions of* m *and* n *respectively, so that* $0 \leqslant m_i(d), n_i(d) < q^d$.

In particular, the binomial is zero modulo $\wp$ *if and only if the* q*-degree of* $n_i(d)$ *is greater than the* t*-degree of* a_i*, for some* i.

Proof. All congruences below are modulo $\wp$ and $0 \leqslant j < d$. By (V) and (III), $\{\begin{smallmatrix}\wp\\ q^i\end{smallmatrix}\} \equiv 0$ for $i \neq d$. Hence by comparing the coefficients in (VII), for $b = \wp$, we have (a)

$$\left\{\begin{matrix} a\wp \\ q^{k+d}\end{matrix}\right\} = \sum_{i+\ell=k+d} \left\{\begin{matrix} a \\ q^i\end{matrix}\right\}\left\{\begin{matrix} \wp \\ q^\ell\end{matrix}\right\}^{q^i} \equiv \left\{\begin{matrix} a \\ q^k\end{matrix}\right\}.$$

On the other hand, we have (b)

$$\left\{\begin{matrix} a \\ q^{kd+j}\end{matrix}\right\} = \sum_{i \geqslant k} \left\{\begin{matrix} a_i\wp^i \\ q^{kd+j}\end{matrix}\right\} \equiv \left\{\begin{matrix} a_k\wp^k \\ q^{kd+j}\end{matrix}\right\} \equiv \left\{\begin{matrix} a_k \\ q^j\end{matrix}\right\},$$

where the first equality is by the $\mathbb{F}_q$-linearity of the binomial coefficient in the top variable and (V), the last by (a) and the middle by using the definition of the binomial and noticing that $a_i\wp^i/L_{kd+j} \equiv 0$, as the numerator has valuation i at $\wp$, and $i > k =$ the valuation of the denominator by (I) and definition of L_i. If we write the base q-expansion of $n_i(d) = \sum n_{ij}q^j$, combining we have

$$\left\{\begin{matrix} a \\ n\end{matrix}\right\} = \prod_i \prod_j \left\{\begin{matrix} a \\ q^{id+j}\end{matrix}\right\}^{n_{ij}} \equiv \prod \prod \left\{\begin{matrix} a_i\wp^i \\ q^{id+j}\end{matrix}\right\}^{n_{ij}} = \prod_i \left\{\begin{matrix} a_i\wp^i \\ n_i(d)q^{id}\end{matrix}\right\} \equiv \prod_i \left\{\begin{matrix} a_i \\ n_i(d)\end{matrix}\right\},$$

as claimed. □

Theorem 3.3. *Let* $\wp$ *be a prime of* A *of degree* d*. Then we have*

$$\left[\begin{matrix} a \\ b\end{matrix}\right] \equiv \prod \left[\begin{matrix} a_i \\ b_i\end{matrix}\right] \mod \wp,$$

where $a = \sum a_i\wp^i$ *and* $b = \sum b_i\wp^i$ *are the base* $\wp$*-expansions of* a *and* b *respectively* (*so that* $\mathcal{N}a_i, \mathcal{N}b_i < \mathcal{N}\wp$) *and when all the binomials are defined.*

In particular, under these conditions the binomial on the left is zero modulo $\wp$ *if and only if* $b_i - a_i$ *is monic for some* i.

Proof. We have

$$\left[\begin{matrix} a \\ b\end{matrix}\right] = \frac{\prod(1 + \{\begin{smallmatrix} b \\ q^i\end{smallmatrix}\})(1 + \{\begin{smallmatrix} a-b \\ q^i\end{smallmatrix}\})}{1 + \{\begin{smallmatrix} a \\ q^i\end{smallmatrix}\}}.$$

In the proof of the last theorem we saw that modulo $\wp$, we have $\{\begin{smallmatrix} a \\ q^{id+j}\end{smallmatrix}\} \equiv \{\begin{smallmatrix} a_i \\ q^j\end{smallmatrix}\}$, so that the product above decomposes over digits base q^d and we see that the left side is the product over i of $[\begin{smallmatrix} a_i \\ b_i\end{smallmatrix}]$ as claimed. □

Remarks 3.4. Note that under the conditions of the theorem, the binomial on the left is $\wp$-integral. We can still get some information by relaxing these conditions (of 'no poles') by interpreting a zero in the numerator or the denominator of the binomial expressions on the right as divisibility by $\wp$ of the numerator or denominator.

4. Results of Wilson type

The classical Wilson/Leibnitz/Lagrange theorem [3] says $(p-1)! \equiv -1 \mod p$, for the classical factorial and p a prime.

Let $\wp$ be a monic prime of degree d. Note that $\mathcal{N}\wp - 1 = q^d - 1 = \sum_{i=0}^{d-1}(q-1)q^i$.

Theorem 4.1. *We have for the first factorial,*

$$(\mathcal{N}\wp - 1)! \equiv (-1)^{d-1} \mod \wp.$$

Proof. We give two proofs. First we observe that the product of non-zero elements of degree less than d is -1 modulo $\wp$ by pairing inverses modulo $\wp$ with elements, as in the classical Wilson proof, since -1 and are the only elements of order dividing two in the cyclic group $(A/\wp A)^*$, which get paired to themselves. Next, note that by (III) of Section 2, we see that $(\mathcal{N}\wp - 1)! = (D_0 \cdots D_{d-1})^{q-1}$ differs from this product by multiplication of signs which contribute $(-1)^{1+q+\cdots+q^{d-1}} = (-1)^d$, since $\prod_{\theta \in \mathbb{F}_q^*} \theta = -1$.

Next we give another proof with formulas. By (II) of Section 2, we have

$$(\mathcal{N}\wp - 1)! - (-1)^{d-1} = \frac{D_d}{L_d} + (-1)^d = [d-1]^{q-1} \cdots [1]^{q^{d-1}-1} + (-1)^d.$$

The proof follows from the observation that for $0 < i < d$, we have $[i]^{q^{d-i}-1} \equiv (t^{q^d} - t^{q^{d-i}})/[i] \equiv -1$ modulo $\wp$, since by Fermat's little theorem $t^{q^d} \equiv t$. □

Theorem 4.2. *If p is odd, and $\theta \in \mathbb{F}_q$, $\theta \neq -1$, we have*

$$\wp \Pi(\wp - 1) \equiv 1/2 \mod \wp, \qquad \Pi(\wp + \theta) \equiv \big(2(1+\theta)\big)^{-1} \mod \wp.$$

Proof. We use (VI). The d-th term of the product gives 2^{-1}. The constant θ or -1 matters only in 0-th term, and $\binom{\wp}{q^i} \equiv 0 \mod \wp$, for $i < d$. This implies the claim easily. □

5. Primality criteria

Now we will study analogs of the classical primality criteria that $(n-1)! \equiv -1 \mod n$ if and only if n is prime, if and only if $\binom{n+m}{n} \equiv 1 \mod n$, for $0 \leqslant m < n$, where the factorial and binomial are classical.

Theorem 5.1. *We have*:

(i) *For $a \in A$, and the first factorial,*

$$(\mathcal{N}a - 1)! \equiv (-1)^{\deg(a)-1} \mod a, \quad \textit{if and only if } a \textit{ is prime}.$$

(ii) *For the second binomial, we have* (*assuming sign conditions giving existence*)

$$\begin{bmatrix} a+b \\ a \end{bmatrix} \equiv 1 \mod a, \quad \textit{for all } b, \mathcal{N}b < \mathcal{N}a, \textit{ if and only if } a \textit{ is prime}.$$

Proof. The if part of (i) is just the Wilson theorem analog above. Conversely, if a is not prime, it has a factor of degree less than $\deg a$, which thus divides $(\mathcal{N}a - 1)!$ by (III) of Section 2, and so cannot divide the factorial ± 1. This proves (i).

Let $\deg a = d$ and $\deg b = \ell$. Then by (VI) of Section 2,

$$\left[\begin{smallmatrix} a+b \\ a \end{smallmatrix}\right] = \frac{\prod_{i=0}^{d}(1+\{\begin{smallmatrix} a \\ q^i \end{smallmatrix}\})\prod_{i=0}^{\ell}(1+\{\begin{smallmatrix} b \\ q^i \end{smallmatrix}\})}{\prod_{i=0}^{d}(1+\{\begin{smallmatrix} a \\ q^i \end{smallmatrix}\}+\{\begin{smallmatrix} b \\ q^i \end{smallmatrix}\})}.$$

By (V), one has cancellation and all products need only run to ℓ.

Now, if a is prime, then by (III), (IV) (or by (III) and (V)) and the definition of the third binomial, $\{\begin{smallmatrix} a \\ q^i \end{smallmatrix}\}$ is divisible by a, if $i < d$. So modulo a, the first product in the numerator contributes 1 and the second and the denominator are the same, proving if part of (ii). Conversely, if a is not a prime and if k is the degree of the smallest degree prime, say c dividing a, then we use b of degree $\ell = k$. All the lower degree terms cancel as before, but $\{\begin{smallmatrix} a \\ q^k \end{smallmatrix}\}$, which is $e_k(a)/D_k$ by (V) is not zero modulo a, because the only term in the product for the numerator which has a factor common to a is a itself, and c divides the denominator by (II). □

Remarks 5.2. (i) On the other hand, we do not get such a binomial primality criterion for the first binomial. In fact, for it, $\binom{n+m}{n} = 1$, for all $0 \leqslant m < n$, if and only if $n = q^k$, as there is no carry over modulo q. Similarly, for the third binomial, we have with $a \in A_+$, $\{\begin{smallmatrix} a+b \\ \mathcal{N}a \end{smallmatrix}\} = 1$, for $0 \leqslant \mathcal{N}b < \mathcal{N}a$, by (V).

(ii) The converse of last theorem of previous section does not hold, as the conclusion of the theorem holds also e.g., if we replace $\wp$ by composite $a = [1]^2$, when $q = 3$. As explained in the proof, the conclusion then is equivalent by (VI) to $\prod_{i=1}^{\deg(a)-1}(1+\{\begin{smallmatrix} a \\ q^i \end{smallmatrix}\}) \equiv 1$ modulo a. It is easy to see that when $q = 2$ $a = (t^2+t+1)^2$ satisfies this, as modulo a, the terms corresponding to $i = 1, 2, 3$ respectively are congruent to 1, $1 + a/L_2$ and $1 + a/L_3$ respectively. But we need $p \neq 2$. I thank Alejandro Lara Rodriguez for making a search through a's of small degree, using SAGE when $q = 3$ and finding the example above, unique such for degree at most 7. (No example exists of degree at most 6 for $q = 5$.)

6. Refined Wilson theorems

Interestingly, while the product of the reduced system of representatives of smallest positive (monic respectively) modulo p ($\wp$ respectively) is $(p-1)!$ $(((\mathcal{N}\wp - 1)/(q-1))!$ respectively), if we use smallest size representatives, it is $(\pm(p-1)/2)!$ $(\pm(\mathcal{N}\wp - 1)!$ respectively)! Also, while simple counting gives $((p-1)/2)!^2 \equiv (-1)^{(p-1)/2}(p-1)!$, in our case $((\mathcal{N}\wp - 1)/w)!^w = (\mathcal{N}\wp - 1)!$ for all w dividing $q-1$, just from the definitions. Another interesting difference is that we have the same $\mathcal{N}\wp - 1$ for several $\wp$'s (namely of same degree).

While the positive elements smaller than p give reduced system of representatives modulo p, the monic elements of smaller size (degree) than $\wp$ do not give the full reduced system and instead, their product is $D_0 \cdots D_{d-1}$, when the degree of the prime $\wp$ is d. One can ask its congruence class. In fact, if we consider the smallest absolute value size representatives classically the relevant product is $((p-1)/2)!$. For $p \equiv 3 \bmod 4$, it is (see e.g. Hardy–Wright) congruent modulo p to $(-1)^n$, where n is the number of quadratic non-residues less than $p/2$.

So we now investigate

$$S := S_d := S_{q,d,\wp} := \left(\frac{\mathcal{N}\wp - 1}{q-1}\right)! = D_0 \cdots D_{d-1} \mod \wp.$$

We have proved that S is $q-1$-th root in $(A/\wp A)^*$ of $(-1)^{d-1}$. But which one? Let us start with some trivial observations.

(i) If $d = 1$ or $q = 2$, then $S = 1$.
(ii) If $p = 2$ or d is odd, then $S \in \mathbb{F}_q^*$. On the other hand, $q = 3$, $d = 2$, $\wp = t^2 + 1$, then $S = t$.
(iii) If d is odd, $((\mathcal{N}\wp - 1)/2)! = S^{(q-1)/2}$ (which is S, if $q = 3$) is ± 1, closer to the classical case.

(iv) If $q=3$ and d odd, then -1 is a quadratic non-residue modulo $\wp$, and so parallel to the classical case, by the same argument, $S=(-1)^n$, where n is the number quadratic non-residues modulo $\wp$ among monics of degree less than d.

(v) If $\wp \in \mathbb{F}_{p^r}[t] \subset \mathbb{F}_q[t]$, and $p=2$ or d is odd, then $S \in \mathbb{F}_{p^r}[t] \cap \mathbb{F}_q^* = \mathbb{F}_{p^r}^*$. In particular, $S=1$, if $p=2$, $r=1$. For example, if $\wp = t^2+t+1$ and $q=2^s$, with s odd, then $S=1$.

Theorem 6.1. *Let $\theta, r \in \mathbb{F}_q^*$. The monic primes $\wp(t)$ for which $S=r$ and those for which $S=r/\theta^{d(d-1)/2}$ are in bijection via $\wp(t) \leftrightarrow \wp(\theta t)/\theta^d$.*

If $\gcd(q-1, d(d-1)/2)=1$, then the primes $\wp$ of degree d are equidistributed in each congruence class $S=r$, as r runs through $q-1$-th roots of $(-1)^{d-1}$.

Proof. Note that if we replace t by θt, $[n]$ gets replaced by $\theta[n]$, and so noting that $q \equiv 1 \bmod q-1$, we see that $D_0 \cdots D_{d-1} = [d-1][d-2]^{1+q} \cdots [1]^{1+q+\cdots+q^{d-2}}$ gets multiplied by $\theta^{1+2+\cdots+(d-1)} = \theta^{d(d-1)/2}$ proving the first claim. Given the gcd condition, as θ runs through all elements of $\mathbb{F}_q^*$, so does $\theta^{d(d-1)/2}$, proving the second claim. □

Remarks 6.2. We can derive many special conclusions. For example, if $d \equiv 3 \bmod 4$, by choosing $\theta=-1$, we see that primes are equidistributed in $S=r$ and $S=-r$.

Theorem 6.3. (1) *Let $\theta \in \mathbb{F}_q$. If $S_{q,d,\wp(t)} = r(t)$, then $S_{q,d,\wp(t+\theta)} = r(t+\theta)$.*

In particular, if $p=2$ or d odd, then

$$S_{q,d,\wp(t)} = S_{q,d,\wp(t+\theta)}.$$

(2) *Let d be odd or $p=2$, so that S can be considered in $\mathbb{F}_q$. Let σ be an automorphism of $\mathbb{F}_q$. Then $S^{\sigma}_{q,d,\wp} = S_{q,d,\wp^{\sigma}}$. In particular, primes are equidistributed in all congruence classes in a $Gal(\mathbb{F}_q/\mathbb{F}_p)$ orbit.*

Proof. Since $[n] = t^{q^n} - t = (t+\theta)^{q^n} - (t+\theta)$, and D_i's are the products of these, the first statement follows. When $p=2$, or d is odd, then as we have seen $r \in \mathbb{F}_q^*$, so that $r(t) = r(t+\theta)$ and the conclusion (1) follows. To see (2), we have only to note that $D_0 \cdots D_{d-1} \in \mathbb{F}_p[t]$. □

Remarks 6.4. Sometimes, $\wp(t+\theta) = \wp(t)$. For example, if $q=p$ and $\wp = \wp_a$ defined below.

Theorem 6.5. *If d is odd and not divisible by p, then the number of primes of degree d for which S is in a particular congruence class r is a multiple of q.*

Proof. The product P_r of primes $\wp$ of degree d for which $S \equiv r$ modulo $\wp$ is the greatest common divisor of $[d]$ and $D_1 \cdots D_{d-1} - r$, and thus a polynomial (say of degree k) in $[1]$ with $\mathbb{F}_q$-coefficients. Hence, the number $N_r := \deg(P_r)/d = q(k/d)$ of such primes is a multiple of q by the hypothesis. □

Remarks 6.6. This q-divisibility makes one wonder whether there is any $\mathbb{F}_q$-vector/affine space structure lurking behind.

7. Congruences modulo prime powers

The usual proof of the Wilson theorem (that the product of elements in $(\mathbb{Z}/p\mathbb{Z})^*$ is -1) generalizes immediately to the proof of well-known fact that the product of elements in a finite abelian group is the product of its elements of order 2, and is thus 1 if there is more than one element of order 2 and is the element of order 2 otherwise. Hence, the product for $(\mathbb{Z}/p^n\mathbb{Z})^*$ is -1 for odd p or $p^n=4$ and 1 otherwise, while for $(A/\wp^n A)^*$ it is -1 unless $q=2$, $\deg \wp = 1$ and $n=2,3$. See [6, p. 7] for more details.

We ask now when does the Wilson type congruence works modulo higher power. Note $(5-1)! \equiv -1 \bmod 5^2$.

Theorem 7.1. *Let $q = p$, $a \in \mathbb{F}_q^*$, so that $\wp_a := t^p - t - a$ is prime in A. We have*

$$[1][2]\cdots[p-1] \equiv -1 \mod \wp_a^{q-1}, \qquad (\mathcal{N}\wp_a - 1)! \equiv 1 \mod \wp_a^{q-1}.$$

Proof. Modulo such $\wp := \wp_a$, we have $[1] \equiv a$, so that $[n] \equiv [1]^{p^{n-1}} + \cdots + [1] \equiv an$ implying $[1][2]\cdots[p-1] \equiv a^{p-1}1 * 2 \cdots (p-1) \equiv -1$, by the usual Fermat and Wilson theorems!

In fact, $[1] = \wp + a$, $[2] = \wp^p + \wp + 2a$ etc. implies $[n] \equiv \wp + na \bmod \wp^p$. So modulo $\wp^p$, we have $[1][2]\cdots[p-1] \equiv \prod(\wp + na) \equiv \prod_{\theta \in \mathbb{F}_q^*}(\wp + \theta) \equiv \wp^{p-1} - 1$, proving the first claim, as well as the fact that the power of $\wp$ cannot be improved.

From the first paragraph, we also see that $[p-1]^p \cdots [1]^{p^{p-1}} \equiv -1 \bmod \wp^p$, so dividing by the first claim, we get the second claim that $(\mathcal{N}\wp - 1)! = [p-1]^{p-1}[p-2]^{p^2-1}\cdots[1]^{p^{p-1}-1} \equiv 1 \bmod \wp^{p-1}$. □

Remarks 7.2. If $q = 2^s$ and $d = 2$, then $\wp || (\mathcal{N}\wp - 1)!$, as is seen from $[2] = [1]^q + [1] = \prod([1] + \theta)$, where θ runs through elements of $\mathbb{F}_q$. This also shows directly that S is equidistributed in $\mathbb{F}_q^*$ in this case.

Theorem 7.3. *We have, for the first binomial,*

$$\binom{\mathcal{N}\wp^k n}{\mathcal{N}\wp^k m} \equiv \binom{n}{m} \mod \wp^{v(n)+q-1}.$$

Proof. By (I), $\wp$ divides $[r]$ if and only if d divides r. Again by (I), $\wp^{q^r}$ divides $[d]^{q^r} = [r+d] - [r]$. If further d divides r, then $[r+d]/\wp \equiv [r]/\wp \bmod \wp^{q^r-1}$.

As explained in the proof of Lucas theorem for the first factorial, if there is no carry over in $m + (n-m)$, then both sides are one. Otherwise carry over produces products of consecutive brackets at the carry over places. More precisely, let k (r respectively) be smallest such that n_k (m_r respectively) is non-zero. If $r < k$, this produces $[k]\cdots[r+1]$. By the two observations above, it is congruent to $[k+d]\cdots[r+1+d]$ modulo $s := \lfloor k/d \rfloor - \lfloor r/d \rfloor + q^{r+1} - 1$-th power of $\wp$. Now $v(n) = \lfloor k/d \rfloor$ and $s \geqslant v(n) + q - 1$. Any other $[a]$ occurring via carry over (e.g. if $r \geqslant k$) has $a \geqslant k$ and thus $[a+d] \equiv [a] \bmod \wp^{q^k}$ and $q^k \geqslant v(n) + q - 1$. □

Remarks 7.4. The case $n = q$, $m = 1$, $\wp = t$ already shows that the power in congruence is the best possible in general. But it can be improved with more information as below.

Theorem 7.5. *We have, for the first binomial,*

$$\binom{\mathcal{N}\wp n}{\mathcal{N}\wp m} \equiv \binom{n}{m} \mod \wp^w,$$

where $w = \max(0, \lfloor k/d \rfloor - \lfloor r/d \rfloor) + q^{\max(r,u)+1} - 1$, where $q^k || n$, $q^r || m$, $q^u || m - n$. (Note $\lfloor k/d \rfloor = v(n)$ and $\lfloor r/d \rfloor = v(m)$.)

Proof. The proof follows the same ideas as in the previous proof, so we just sketch the changes and the cases. (i) If $r < k$, then $u = r$ and the carry over produces $[k]\cdots[r+1]$, which is divisible by the 'difference of the floors' power of $\wp$ as before and when divided by them reduces the power by one, as in the previous proof, leading to power difference of floors $+q^{r+1} - 1$ as before and as claimed. (ii) If $r > k$, then $u = k$ and only possible carry overs lead $[a]$'s with $a \geqslant r$ leading congruences to

$q^{r+1}-1$ power as claimed. (iii) $r=k$ and $u=r=k$. This leads to same situation as in (ii). Finally, in case (iv) $r=k$, $u>r$, we use symmetry $\binom{n}{m}=\binom{n}{n-m}$ and reduce to the previous case leading to $q^{u+1}-1$-th power as claimed. □

Remarks 7.6. Good example, where the reader can profitably make direct check very easily is $\wp=t$, $n=q^k$ and $m=q^j$.

Theorem 7.7. *We have, for the third binomial, denoting valuation at $\wp$ by $v_\wp$, and $v:=v_\wp(a)$, we have*

$$\left\{ \begin{matrix} a_\wp \\ q^k\mathcal{N}_\wp \end{matrix} \right\} \equiv \left\{ \begin{matrix} a \\ q^k \end{matrix} \right\} \mod \wp^{\max(q^{k+1}, v-\lfloor k/d \rfloor)}.$$

Proof. Comparing the coefficients in (VII), we get

$$\left\{ \begin{matrix} a_\wp \\ q^{k+d} \end{matrix} \right\} = \sum_{j+\ell=k+d} \left\{ \begin{matrix} a \\ q^j \end{matrix} \right\} \left\{ \begin{matrix} \wp \\ q^\ell \end{matrix} \right\}^{q^j} = \sum_{j+\ell=k+d} \left\{ \begin{matrix} \wp \\ q^\ell \end{matrix} \right\} \left\{ \begin{matrix} a \\ q^j \end{matrix} \right\}^{q^\ell}.$$

Now the definition of the third binomial and (II), (III) immediately gives that $v_\wp(\{ \begin{smallmatrix} \wp \\ q^j \end{smallmatrix} \})=1$, if $j<d$, so that the first sum expression gives

$$\left\{ \begin{matrix} a_\wp \\ q^k q^d \end{matrix} \right\} \equiv \left\{ \begin{matrix} a \\ q^k \end{matrix} \right\} \mod \wp^{q^{k+1}},$$

irrespective of v. (Using digit expansions, we can replace q^k in the two binomials by any of its multiple in the congruence above.) But if this valuation is big, we can do better by using the second sum expression instead.

First note that by Fermat's little theorem and (IV), the term for $\ell=d$ is congruent to $\{ \begin{smallmatrix} a \\ q^k \end{smallmatrix} \}$. Now if we look at terms in the definition of the third binomial $\{ \begin{smallmatrix} a \\ q^k \end{smallmatrix} \}$, they have valuations $q^j v - v_\wp(D_j) - q^j \lfloor (k+j)/d \rfloor$, which have unique minimum at $j=0$, if ('the minimum') $v-\lfloor k/d \rfloor$ is $\geqslant q^{k+1}$, which is the only case of interest for us. This gives the valuation of $\{ \begin{smallmatrix} a \\ q^k \end{smallmatrix} \}$ and the second sum expression thus gives the required congruence to w-th power, where $w=1+\min(q^{d-j}(v-\lfloor (k+j)/d \rfloor))$, and $1 \leqslant j \leqslant d$. Again under our assumption that $v-\lfloor k/d \rfloor \geqslant q^{k+1}$, the minimum is unique at $j=d$ and is $v-\lfloor k/d \rfloor$ as claimed. □

Remarks 7.8. (i) Note that both the sides of the congruence are zero, for $k>\deg(a)$.

(ii) The sum formula in the definition of the third binomial, together with $\{ \begin{smallmatrix} \wp \\ q^d \end{smallmatrix} \}=1$ lead to $\wp/L_d \equiv (-1)^d$ modulo $\wp^q$, if $d>1$, and modulo $\wp^{q-1}$, if $d=1$. By (I) and (IV), this can be reformulated as interesting congruence saying that the monic least common multiple of all, except $\wp$, elements of degree d, which is also equal to the product of $P^{\lfloor d/\deg(P) \rfloor}$ over monic primes $P \neq \wp$ (of degree at most $\wp$ only matter) is congruent to $(-1)^d$ modulo $\wp^q$ (respectively $\wp^{q-1}$) if $d>1$ (respectively $d=1$).

Let us provide an analog of the theorem [3] on the classical factorial that $(np)! \equiv n!(p!)^n \bmod p^{n+3}$.

Theorem 7.9. *We have for the first factorial,*

$$(n\mathcal{N}_\wp)! \equiv n!\big((\mathcal{N}_\wp)!\big)^n \mod \wp^{n+q}.$$

Proof. Let $n = \sum n_i q^i$ be the base q expansion. Hence

$$(n\mathcal{N}_\wp)! = \prod D_{i+d}^{n_i} = \prod \left([d+i][d+i-1]^q \cdots [d+1]^{q^{i-1}}\right)^{n_i} D_d^{\sum n_i q^i}.$$

Now, by (III), $\wp^n$ divides D_d^n and when you divide out this $\wp$ power, we use $[d+j] \equiv [j] \bmod \wp^{q^j}$. Hence the claim follows, when we notice that $i = 0$ gives identity, so, in general, the minimum power in the divided out congruence holds for q-th power of $\wp$ corresponding to $i = 1$. □

The special case $n = q$ shows that the power in the congruence is best possible in general.

8. Higher powers and Bernoulli numbers

See [3] and [5] (and its review on MathSciNet by Evans) for references for many more results (some mentioned below) by Lagrange, Wolstenholme, Ferrers, Glaisher, Carlitz etc. generalizing these results and on congruences modulo higher powers of primes for the classical binomial.

In particular, congruences analogous to those in Section 7 work, for given m, n, to higher power of a prime p if and only if p divides Bernoulli number $B_{p-3} = B_{p-1-2} \in \mathbb{Q}$. In fact, for the usual binomial coefficients and factorials, (a) $\binom{np}{mp}/\binom{n}{m} \equiv 1 + mn(m-n)B_{p-3}p^3/3 \bmod p^{t+4}$, where $p \geqslant 5$ and $p^t || mn(m-n)$. Carlitz proved this with p^{t+4} replaced by p^4. Its often quoted immediate consequences are (b) $\binom{np-1}{p-1} \equiv 1 - n(n-1)p^3 B_{p-3}/3 \bmod p^4$ and (c) $(np)!/(n!(p!)^n) \equiv 1 - (n^3-n)p^3 B_{p-3}/9 \bmod p^4$. Carlitz also proved (d) $\binom{p-1}{(p-1)/2} \equiv (-1)^{(p-1)/2} 4^{p-1}(1 + p^3 B_{p-3}/12) \bmod p^4$.

Let us look at the $\mathbb{F}_q[t]$ situation. For $n = q+1$, $m = 2$ the congruence in the case (Theorem 7.3) of the first binomial reduces to $[d+1] \equiv [1]$ and q is the exact power of $\wp$ dividing $[d+1] - [1] = [d]^q$ for any $\wp$ of degree d, by (I). So there is no extra divisibility, at least in the full generality of the classical case. In the case (Theorem 7.7) of the third binomial also, if, for example, we take $a = t$, then the power of $\wp$ in the displayed congruence in the proof is the best by argument there, for any $\wp \neq t$. Hence there is no extra divisibility as in (a). As for (b), no carry over implies that for the first binomial, we have $\binom{n\mathcal{N}_\wp - 1}{\mathcal{N}_\wp - 1} = 1$, in fact. (Note that immediate argument for deducing (b) from (a) in the classical case fails in this case.) Analog of (d): For the first binomial, $\binom{\mathcal{N}_\wp - 1}{(\mathcal{N}_\wp - 1)/(q-1)}$ is identically one, again for no carry over reason. Similarly, we do not get extra divisibility for (c).

On the other side with Bernoulli, see [6, Sec. 4.16 and 5.3.9] or [4] for more on these Bernoulli–Carlitz numbers $B_n \in \mathbb{F}_q(t)$ and many analogies they satisfy, such as their generating function, occurrence in special Carlitz zeta 'even' value, analog of the von-Staudt theorem etc. Analog of B_n/n is then $B_n(n-1)!/n!$ [6, Sec. 4.16], where the factorial is the first factorial. In this case, no nice functional equation is known for the Carlitz–Goss zeta function [4,6], so that there are also Bernoulli–Goss numbers $\beta(n)$ (these, rather than Bernoulli–Carlitz numbers, satisfy analogs of Kummer congruences leading to $\wp$-adic interpolation) coming from the special values at negative integers.

Now, let us recall the Carlitz evaluation [6, Thm. 4.16.1] of the special 'Bernoulli–Carlitz numbers'

$$B_{q^h - q^i} = \frac{(-1)^{h-i}(q^h - q^i)!}{L_{h-i}^{q^i}}.$$

From the evaluation and (I), we see that $\wp$ never divides the Bernoulli–Carlitz number $B_{\mathcal{N}_\wp - q} = B_{(\mathcal{N}_\wp - 1) - (q-1)} \in K$.

We have not yet fully investigated what happens for them in general, but we have checked that for $q = 3$, $\wp$ does not divide $\zeta(1 - (q^d - q))$, if $d \leqslant 5$. On the other hand, out of 8 primes of degree 3 in $\mathbb{F}_q[t]$, two divide the Bernoulli–Goss number $\beta(3^3 - 3)$, with close connection to the class group component related to B_{3^3-3}, via analogs of the Herbrand–Ribet [6, Theorems 5.2.4, 5.3.8], [4].

Next, let us look at the Lagrange, Wolstenholme, Ferrers, Glaisher results generalizing Wilson's theorem to other elementary symmetric functions: If we write $(x-1)(x-2)\cdots(x-p+1) = x^{p-1} - A_1x^{p-2} + \cdots + A_{p-1}$, then modulo p (for indices strictly between 0 and $p-1$),

$$\text{(i) } A_r \equiv 0, \qquad \text{(ii) } A_{2r}/p \equiv -B_{2r}/(2r), \qquad \text{(iii) } A_{2r+1}/p^2 \equiv (2r+1)B_{2r}/(4r).$$

The Carlitzian analog would be $\prod(x-a) = \sum_{i=0}^{d} x^{q^{d-i}-1}F_{q^d-q^{d-i}}$, where the product is over non-zero polynomials a of norm less than $\mathcal{N}\wp$. Thus by the definition of the third binomial and (V), we have

$$F_{q^d-q^{d-i}} = \frac{D_d(-1)^i}{D_{d-i}L_i^{q^{d-i}}}.$$

So by (I)–(IV), these coefficients are divisible by $\wp$, but not its higher powers, in analogy as well as contrast with the classical case mentioned above. Comparing the Bernoulli–Carlitz evaluation above, using an identity similar to (II), an easy calculation shows that we have, for $0 < i < d$,

$$F_{q^d-q^{d-i}}/\wp = (L_d/\wp)B_{q^d-q^{d-i}}/L_{d-i} \equiv (-1)^d B_{q^d-q^{d-i}}/L_{d-i},$$

where the last congruence is modulo $\wp^q$ (or $\wp^{q-1}$, if $d=1$) and follows by Remark 7.8(ii).

9. Further questions, observations and partial results

(A) Since the second congruence in Theorem 7.1 works with the first power of $\wp$ for all $\wp$, it raises similar question for the first congruence. By an argument similar to Euclid's argument for infinitude of primes, by (I), $[1]\cdots[s-1]+1$ can only be divisible by primes of degree $\geqslant s$ and we are asking when it is divisible by the lowest possible degree s. For $s = p = q$, it seems, but not yet proved that the only primes which enter are the $\wp_a$'s identified in Theorem 7.1.

Small amount of data that we calculated shows that it works for some other primes (what is their characterization?), but only in degrees divisible by the characteristic p. More precisely, it suggests the guess that the greatest common divisor G of $A := [1]\cdots[s-1]+1$ and $B := [s]$ is non-trivial, only if $p|s$. Here is the proof for $s \leqslant 4$ and all q:

For $s = 1$ it is vacuously true. For $s = 2$, it follows since $D_1 = [1]$ is congruent to $q-1$-th root of -1, and is thus congruent to one only if $p = 2$. For $s = 3, 4$, it follows also by the following calculation. (We speculate, but cannot prove yet, that the method of this proof generalizes to all s.)

Let $x := [1]$, then $[s] = x^{q^s-1} + \cdots + x^q + x$, so that gcd G of A, B is a polynomial in x. If G is a polynomial in x of degree $w > 0$ prime to s, then G is a polynomial of degree wq in t, on the other hand its prime factors are all of degree s. So wq is a multiple of s, hence p divides s.

For $s = 2$, $A^q - B = x - 1$.

For $s = 3$, $x^qB - A^q - A = -x^2 - 2$ divisible by G, so that $w = 1$ or 2.

For $s = 4$, let $C = A^q - x^q(x^{q^2} + x^q)B$, $D = (A-C)/x^2$, $E = B - D^q = -x^{q^2} + x$, $F = x^{q+1}E + C$, and $G = F(x^{q^2} + x^q + x)F - x^qA = x^{q^2} + x$. Then $E + G = 2x$, so $w = 1$, unless $p = 2$.

(B) The next unresolved question is what the distribution of primes corresponding to the different possibilities for S in Section 6 is, when the hypothesis of Theorem 6.1 does not apply. Here are some observations from the small numerical data gathered by calculating P_r and N_r, the number of primes corresponding congruence class r (see proof of Theorem 6.5 for the notation), using maxima.

(i) For $d = 3$, we focus on the primes $q \leqslant 61$ and $q \equiv 1$ modulo 3 (not fully handled by Theorem 6.1) and give the vector of entries N_r/q (see Theorem 6.5) corresponding to $1 \leqslant r \leqslant (q-1)/2$ (this range is enough by Remark 6.2) is given by

$q = 7,\ [3, 4, 1];$ $\qquad q = 13,\ [3, 4, 4, 7, 3, 7];$ $\qquad q = 19,\ [9, 4, 4, 7, 4, 7, 9, 9, 7];$

$q = 31,\ [12, 12, 13, 12, 7, 13, 13, 12, 7, 7, 7, 13, 7, 13, 12];$

$q = 37$, [9, 16, 13, 13, 13, 9, 13, 9, 16, 9, 9, 16, 13, 9, 16, 16, 16, 13];

$q = 43$, [12, 12, 19, 12, 19, 19, 13, 12, 13, 19, 12, 19, 13, 13, 13, 12, 13, 13, 19, 19, 12];

$q = 61$, [21, 16, 21, 25, 16, 16, 16, 21, 21, 25, 21, 25, 16, 25, 16, 16, 25, 16, 25, 21, 16, 16, 21, 21, 25, 25, 21, 21, 25, 25].

Here, all the repeat entries can be explained by the bijection in Theorem 6.1.

(ii) Let $d = 3$ and $r = 1$. For $q = 3^n$, N_1 is $q(q+1)/3$ (and thus not a multiple of q), at least for $n \leqslant 4$. For $q = 4, 16, 64, 256$ N_1/q is $3, 3, 27, 75$ respectively and for $q = 25, 49$ it is $12, 21$ respectively.

(iii) For $q = 4$, $d = 4$, $S = 1$ class is empty and the primes are equidistributed in classes for $S = \zeta_3$ and $S = \zeta_3^2$ (equidistribution is in accordance with Theorem 6.3(2)).

An independent characterization of the distribution of these numbers and of the primes themselves in congruence classes would be interesting.

References

[1] Manjul Bhargava, P-orderings and polynomial functions on arbitrary subsets of Dedekind rings, J. Reine Angew. Math. 490 (1997) 101–127.
[2] Manjul Bhargava, The factorial function and generalizations, Amer. Math. Monthly 107 (9) (2000) 783–799.
[3] Leonard Dickson, History of the Theory of Numbers (1919), vol. I, Dover edition, 2005, Chapter 9.
[4] David Goss, Basic Structures of Function Field Arithmetic, Ergeb. Math. Grenzgeb. (3) (Results in Mathematics and Related Areas (3)), vol. 35, Springer-Verlag, Berlin, 1996.
[5] Andrew Granville, Arithmetic properties of binomial coefficients I binomial coefficients modulo prime powers, in: Organic Mathematics, Burnaby, BC, 1995, in: CMS Conf. Porc., vol. 20, Amer. Math. Soc., Providence, RI, 1997, pp. 253–276.
[6] Dinesh S. Thakur, Function Field Arithmetic, World Scientific Publishing Co. Inc., River Edge, NJ, 2004.